Serial No.: 09/716,682 -2-

## **Amendments to the Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application:

- 1. (Currently amended) A security method for controlling access to a function of a digital television receiver, comprising the steps of:
  - (a) providing a software application at the receiver; said software application being executable in response to an execution command;
- (b) <u>receiving providing</u> data <u>at the receiver from a headend, said data defining a condition of</u> the receiver under which access to the receiver function by the software application is permitted;
- (c) receiving information at the receiver from the headend, said information defining a security policy for said software application which contains a set of permissions for said software application;
- (ed) providing a control signal for requesting access to the receiver function upon execution of said software application;
- (de) in response to said control signal, determining whether an associated the security policy for of the software application contains a permission for the software application to access the receiver function;
  - (ef) if said security policy contains said permission:
  - (i) determining whether said condition of the receiver is met by data indicative of a current state of the receiver;
  - (ii) allowing the software application to access the receiver function if the condition is met; and
  - (iii) preventing the software application from accessing the receiver function if the condition is not met; and
- (fg) if said security policy does not contain said permission, preventing the software application from accessing the receiver function.

Serial No.: 09/716,682

2. (Original) The method of claim 1, wherein:

said condition indicates a conditional access state of the receiver.

3. (Original) The method of claim 2, wherein said conditional access state comprises at least one of:

a blackout state;

a pay-per-view state; and

an authorization state.

4. (Original) The method of claim 1, wherein:

said condition indicates a user state of the receiver.

5. (Original) The method of claim 4, wherein said user state comprises at least one of:

user preferences;

a user password; and

a user identifier.

6. (Original) The method of claim 5, wherein:

said condition indicates at least one of a time, date, and day.

7. (Original) The method of claim 1, wherein:

said condition is defined, at least in part, by said software application.

8. (Original) The method of claim 1, wherein:

said condition indicates that one of a channel and a group of channels is tuned by the receiver.

9. (Original) The method of claim 1, wherein:

the software application is downloadable to the receiver via a broadband television network.

Serial No.: 09/716,682

- 10. (Cancelled).
- 11. (Original) The method of claim 1, wherein: the software application comprises a Java code.
- 12. (Original) The method of claim 1, wherein: the execution command is initiated by a user.
- 13. (Original) The method of claim 1, wherein: the permission is associated with a user of the receiver.
- 14. (Original) The method of claim 1, wherein:
  the condition is embedded in code that defines the permission.
- 15. (Original) The method of claim 1, wherein:

  the software application is multicast to a receiver population including said receiver.
- 16. (Cancelled).
- 17. (Currently amended) A security apparatus for controlling access to a function of a digital television receiver, comprising:
  - (a) means for providing a software application at the receiver; said software application being executable in response to an execution command;
- (b) means for providing receiving data at the receiver from a headend, said data defining a condition of the receiver under which access to the receiver function by the software application is permitted;
  - (c) means for receiving information at the receiver from the headend, said information

defining a security policy for said software application which contains a set of permissions for said software application;

- (ed) means for providing a control signal for requesting access to the receiver function upon execution of said software application;
- (de) means for determining, in response to said control signal, whether an associated the security policy of <u>for</u> the software application contains a permission for the software application to access the receiver function;
- (ef)(i) means for determining whether said condition of the receiver is met by data indicative of a current state of the receiver when said security policy contains said permission;
- (ef)(ii) means for allowing the software application to access the receiver function if the condition is met, and when said security policy contains said permission;
- (ef)(iii) means for preventing the software application from accessing the receiver function if the condition is not met, and when said security policy contains said permission; and
- (fg) means for preventing the software application from accessing the receiver function if said security policy does not contain said permission.